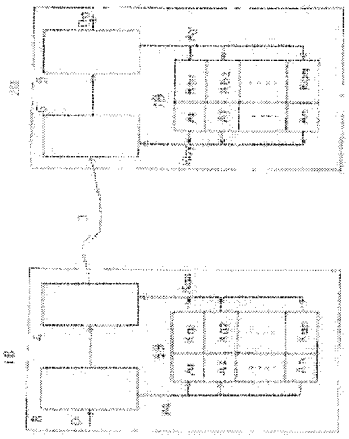
DATA TRANSMISSION METHOD

Publication number: JP4072841 (A)
Publication date: 1992-03-06
Inventor(s): MATSUDA YOSHIMI
Applicant(s): NISSIN ELECTRIC CO LTD
Classification:
- international: ***H04L9/16; H04L9/06; H04L 9/14; H04L9/36;*** **H04L9/14; H04L9/06; H04L9/36;** (IPC1-7): H04L9/06; H04L9/14
- European:
Application number: JP19900185077 19900712
Priority number(s): JP19900185077 19900712

Also published as:
JP3070072 (B2)

Abstract of **JP 4072841 (A)**

PURPOSE:To disable decoding of a cryptographic code when a key data is stolen at the write of, e.g. a cryptographic key management section and a decoding key management section by revising a cryptographic key and a decoding key so as to be always made correspondent interlockingly during data transmission. CONSTITUTION:A cryptographic key management section 5B and a decoding key management section 7B store plural cryptographic keys and decoding keys and any of the cryptographic keys of the management section 5B is selected at random for each cryptographic processing of a prescribed number of transmission data to revise a decoding key periodically at random.; Moreover, a relevant decoding key of the management section 7B is selected for each decoding of a prescribed number of received data and the decoding key is revised at random in interlocking with the revision of the cryptographic key. Thus, the data transmission of the cryptographic processing system is implemented while revising the cryptographic key automatically at random during the transmission and the decoding of a cryptographic code is almost disabled and the reliability of security is improved.



⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−72841

⑤Int. Cl.[5]　識別記号　庁内整理番号　⑬公開　平成4年(1992)3月6日

H 04 L 9/06
9/14

7117−5K　H 04 L 9/02　Z

審査請求　未請求　請求項の数 1　(全5頁)

⑭発明の名称　データ伝送方法

⑳特　願　平2−185077
㉒出　願　平2(1990)7月12日

⑫発明者　松田　義巳　京都府京都市右京区梅津高畝町47番地　日新電機株式会社内
⑪出願人　日新電機株式会社　京都府京都市右京区梅津高畝町47番地
⑭代理人　弁理士　藤田　龍太郎

明細書

1　発明の名称

データ伝送方法

2　特許請求の範囲

① 送信側により数字，文字等の送信データを暗号鍵を用いて順次に暗号化して送信し、受信側により暗号化された受信データを復号鍵を用いて順次に復号化するデータ伝送方法において、

送信側に複数の暗号鍵を保持した暗号鍵管理部を設けるとともに、受信側に前記暗号鍵管理部の各暗号鍵に対応する複数の復号鍵を保持した復号鍵管理部を設け、

暗号化する一定数の送信データ毎に誤り訂正符号の生成等に基づいて送信側のランダム選択信号を形成し、

該送信側のランダム選択信号に基づき、前記暗号鍵管理部の各暗号鍵を前記一定数の送信データの暗号化毎にランダムに選択して暗号化の鍵を周期的にランダムに変更し、

一定数の受信データの復号化毎に誤り訂正符号の生成等に基づいて前記送信側のランダム選択信号に相当する受信側のランダム選択信号を形成し、

該受信側のランダム選択信号に基づき、前記復号化鍵管理部の各復号鍵を前記一定数の受信データの復号毎にランダムに選択し、復号化の鍵を前記暗号化の鍵の変更に連動してランダムに変更する

ことを特徴とするデータ伝送方法。

3　発明の詳細な説明

〔産業上の利用分野〕

本発明は、数字，文字等のデータを送信側の暗号鍵，受信側の復号鍵を用いた暗号化方式で暗号化して伝送するデータ伝送方法に関する。

〔従来の技術〕

従来、この種鍵を用いた暗号化方式のデータ伝送は、第2図に示すように送信側の暗号化装置(1A)と受信側の復号化装置(2A)とを無線又は有線の伝送路(3)で結合して行われる。

そして、暗号化装置(1A)は暗号化部(4)及びメモリ等で形成された暗号鍵管理部(5A)を備え、この

(1)　(2)

管理部(5A)は上位装置又は人手の書込みによって与えられた特定データの１個の暗号鍵を保持する。

また、復号化装置(2A)は復号化部(6)及びメモリ等で形成された復号鍵管理部(7A)を備え、この管理部(7A)は暗号鍵に対応する1個の復号鍵を保持する。

そして、暗号化装置(1A)の数字，文字等の送信データDiは順次に暗号化部(4)に送られ、この暗号化部(4)により暗号鍵管理部(5A)の暗号鍵を用いて暗号化される。

この暗号化は、例えば送信データDiと暗号鍵のデータKaとの四則演算により施される。

そして、暗号化された送信データDiは、伝送路(3)を介して復号化装置(2A)に順次に伝送される。

つぎに、復号化装置(2A)においては、暗号化された送信データDiが受信データとして順次に復号化部(6)に供給される。

そして、復号化部(6)により、復号鍵管理部(7A)の復号鍵を用いて受信データが復号化され、送信データDiと同一の復号データDoが再生される。

(3)

なお、復号化は、例えば復号鍵のデータKbを用いた暗号化の逆演算により施される。

〔発明が解決しようとする課題〕

前記従来のデータ伝送方法の場合、暗号鍵，復号鍵が１組だけ用いられるとともに、両鍵の内容（データ）は上位装置又は人手で書換えられない限り変わらない。

そして、暗号化と復号化との鍵の不一致に基づく復号化ミス等を防止するため、少なくともデータ伝送中に両鍵の内容が書換えられて変更されることはなく、通常は両鍵が初めに与えられた内容に固定されて用いられる。

したがって、例えば管理部(5A)，(7A) の書込み時に両鍵それぞれのデータKa，Kb が盗まれたりすると、極めて簡単に暗号解読が行われてデータが盗用され、機密保持の信頼性が低い問題点がある。

本発明は、暗号鍵，復号鍵を周期的に変更し、機密保持の信頼性を向上するようにしたデータ伝送方法を提供することを目的とする。

〔課題を解決するための手段〕

(4)

前記目的を達成するために、本発明のデータ伝送方法においては、送信側に複数の暗号鍵を保持した暗号鍵管理部を設けるとともに、受信側に前記暗号鍵管理部の各暗号鍵に対応する複数の復号鍵を保持した復号鍵管理部を設け、

暗号化する一定数の送信データ毎に誤り訂正符号の生成等に基づいて送信側のランダム選択信号を形成し、

該送信側のランダム選択信号に基づき、前記暗号鍵管理部の各暗号鍵を前記一定数の送信データの暗号化毎にランダムに選択して暗号化の鍵を周期的にランダムに変更し、

一定数の受信データの復号化毎に誤り訂正符号の生成等に基づいて前記送信側のランダム選択信号に相当する受信側のランダム選択信号を形成し、

該受信側のランダム選択信号に基づき、前記復号化鍵管理部の各復号鍵を前記一定数の受信データの復号毎にランダムに選択し、復号化の鍵を前記暗号化の鍵の変更に連動してランダムに変更する。

(5)

〔作　用〕

前記のように構成された本発明のデータ伝送方法の場合、暗号鍵管理部，復号鍵管理部には、従来と異なり、複数の暗号鍵，復号鍵それぞれが保持される。

そして、送信側のランダム選択信号に基づき、一定数の送信データの暗号化毎に暗号鍵管理部の各暗号鍵のいずれか１つがランダムに選択されてつぎの暗号化の鍵になる。

また、送信側のランダム選択信号に相当する受信側のランダム選択信号に基づき、一定数の受信データの復号化毎に、暗号鍵管理部の選択された暗号鍵に対応する復号鍵が復号鍵管理部から選択されてつぎの復号化の鍵になる。

したがって、周期的なランダム選択により、データ伝送中に暗号化の鍵と復号化の鍵とが常に対応するように連動して変更される。

そして、暗号化，復号化の鍵がそれぞれ複数になり、しかも、データ伝送中に両鍵が設定された周期でランダムに変わるため、例えば暗号鍵管理

(6)

部，復号鍵管理部の書込み時に鍵のデータが盗まれても、暗号解読が行えず、機密保持の信頼性が向上する。

〔実施例〕

1実施例について、第1図を参照して説明する。

第1図において、(1B),(2B) は第2図の装置(1A),(1B) に相当する暗号化装置，復号化装置であり、暗号化部(4)，復号化部(6)それぞれを有する。

(8)は暗号化部(4)の前段に設けられた送信側ランダム選択信号形成用の誤り訂正符号生成部、(5B)は第2図の管理部(5A)の代わりに設けられた暗号鍵管理部であり、順次のアドレス$A_1, A_2, \cdots, An$に1番目，2番目，…，N番目の暗号鍵のデータ$Ka_1, Ka_2, \cdots, Kan$を保持する。

(9)は復号化部(6)の後段に設けられた受信データ側ランダム選択信号形成用の誤り訂正符号生成部、(7B)は第2図の管理部(7A)の代わりに設けられた復号鍵管理部であり、順次のアドレス$A_1, A_2, \cdots, An$に管理部(5B)の各暗号鍵それぞれに対応する各復号鍵のデータ$Kb_1, Kb_2, \cdots, Kbn$を保持する。

そして、管理部(5B),(7B) はそれぞれメモリ等で形成され、上位装置又は人手により予め各暗号鍵のデータ$Ka_1 \sim Kan$，各復号鍵のデータ$Kb_1 \sim Kbn$が書込まれる。

また、生成部(8)，(9)は例えばカウンタ機能及びチェックサム方式の誤り訂正符号の生成機能を有する同一構成の誤り訂正符号生成回路により形成され、暗号化部(4)に供給される暗号化前の送信データDi，復号化部(6)から出力された復号化後の受信データすなわち復号データDoそれぞれを一定数M（Mは1，…の整数）計数する毎に、送信側，受信側のランダム選択信号としての誤り訂正符号の信号Ax,Ayそれぞれを生成する。

この誤り訂正符号の信号Ax,Ay は、M個の送信データDi，復号データDoそれぞれのうちの1又は複数個を用いた公知の誤り訂正符号生成で形成され、アドレス$A_1, A_2, \cdots, An$ のいずれかにランダムに変化し、管理部(5B),(7B) の同一アドレスのデータを読出す。

そして、データ伝送が開始されると、装置(1B)，

(2B)のスタート操作等により生成部(8)，(9)が初期化され、信号Ax,Ay が共にアドレスA_1の信号になる。

このとき、管理部(5B)から暗号化部(4)に1番目の暗号鍵のデータKa_1が読出されるとともに、管理部(7B)から復号化部(6)に1番目の復号鍵のデータKb_1が読出され、暗号化の鍵及び復号化の鍵の初期設定が行われる。

そして、生成部(8)を介して暗号化部(4)に供給された送信データDiは、1番目の暗号鍵を用いて暗号化される。

さらに、暗号化された送信データDiは、伝送路(3)を介して復号化装置(2B)に順次に伝送される。

このとき、受信した送信データDiは受信データとして復号化部(6)に供給され、この復号化部(6)により、受信データが1番目の復号鍵を用いて正しく復号化される。

そして、M個の送信データDiが1番目の暗号鍵を用いて順次に暗号化され、一定数の暗号化が終了すると、生成部(8)が新たな誤り訂正符号を生成

して信号Axを変更する。

このとき、信号Axは符号生成に用いられた送信データDiの内容に応じてアドレス$A_1 \sim An$のいずれかにランダムに変化する。

さらに、信号Axの変更に基づき、管理部(5B)から読出される暗号化の鍵のデータKaxは、M番目の送信データDiの暗号化直後に1番目の暗号鍵のデータKa_1から指定されたアドレスの暗号鍵のデータに変わる。

また、前記M個の送信データDiに基づく各受信データが1番目の復号鍵を用いて復号化され、一定数の復号化が終了すると、生成部(9)により、生成部(8)で生成された符号と同一の新たな誤り訂正符号が生成されて信号Ayが変更される。

そして、信号Ayの変更に基づき、管理部(7B)から読出される復号鍵のデータKby も1番目の復号鍵のデータKb_1から指定されたアドレスの復号鍵のデータに変わる。

このとき、信号Ax,Ay が同じアドレスの信号になるため、管理部(7B)から読出される復号鍵は管

理部(5B)から読出される暗号鍵に対応した鍵になる。

したがって、つぎのM個の送信データDiはランダムに選択された新たな暗号鍵を用いて暗号化され、この暗号化に基づくM個の受信データは暗号鍵に応じて変更された復号鍵を用いて復号化される。

以降、M個の送信データDiの暗号化が終了する毎に、暗号化の鍵が管理部(5B)に保持された各暗号鍵のいずれかにランダムに変更される。

また、M個の受信データの復号化が終了する毎に、復号化の鍵も暗号化の鍵の変更に連動して管理部(7B)の対応する復号鍵にランダムに変更される。

そして、データ伝送中に暗号化の鍵が周期的にランダムに変わるため、暗号鍵のデータKa_1～Kan，復号鍵のデータKb_1～Kbnが盗まれても、それらの変更の順序及び周期が全く分らず、暗号解読はほぼ不可能になる。

なお、解読を一層困難にするため、変更の周期

(11)

については、送信データDiのビットパターンの出現状況等を考慮して調整することが望ましい。

そして、回路構成及び送信側，受信側のランダム選択信号の形成手法等は、実施例に限定されるものではない。

〔発明の効果〕

本発明は以上説明したように構成されているため、以下に記載する効果を奏する。

暗号鍵管理部(5B)，復号鍵管理部(7B)に複数の暗号鍵，復号鍵を保持し、送信データの一定数の暗号化毎に管理部(5B)の各暗号鍵のいずれかをランダムに選択して暗号化の鍵を周期的にランダムに変更するとともに、受信データの一定数の復号化毎に管理部(7B)の対応する復号鍵を選択し、復号化の鍵を暗号化の鍵の変更に連動してランダムに変更したため、伝送中に暗号化の鍵を自動的にランダムに変更して暗号化方式のデータ伝送が行え、このとき、暗号解読がほぼ不可能になり、機密保持の信頼性が飛躍的に向上する。

4　図面の簡単な説明

(12)

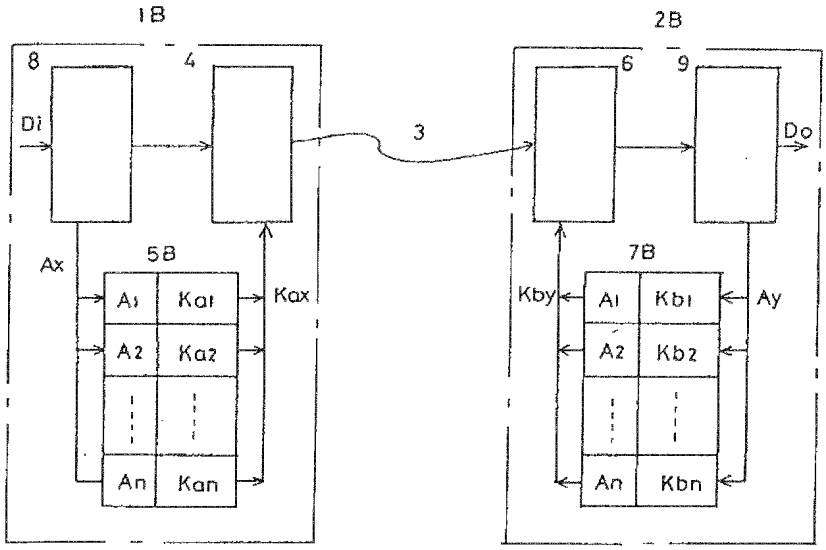
第1図は本発明のデータ伝送方法の1実施例のブロック図、第2図は従来例のブロック図である。

(1B)…暗号化装置、(2B)…復号化装置、(3)…伝送路、(4)…暗号化部、(5B)…暗号鍵管理部、(6)…復号化部、(7B)…復号鍵管理部、(8)，(9)…誤り訂正符号生成部。

代理人　弁理士　藤田　龍太郎

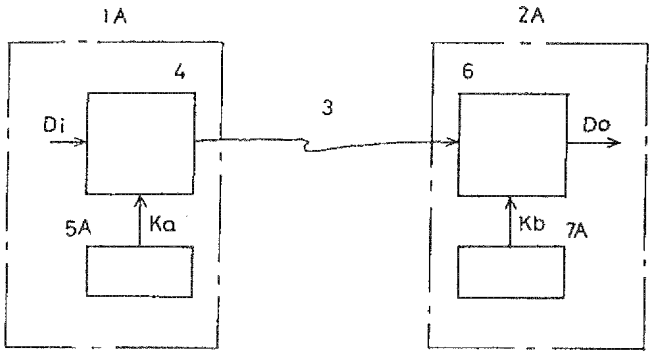
(13)

第 1 図



1B --- 暗号化装置
2B --- 復号化装置
3 --- 伝送路
4 --- 暗号化部
5B --- 暗号鍵管理部
6 --- 復号化部
7B --- 復号鍵管理部
8,9 --- 誤り訂正符号生成部

第 2 図



1A --- 暗号化装置
2A --- 復号化装置
5A --- 暗号鍵管理部
7A --- 復号鍵管理部